REMARKS

Applicant respectfully requests consideration of the subject application as amended herein. This Amendment is submitted in response to the Office Action mailed on January 11, 2008. Claims 1-24 are rejected. In this Amendment, claims 1, 3-6, 8-13, and 15-24 have been amended. Claims 2, 7 and 14 have been canceled. Claims 25-28 have been added. No new matter has been added. Therefore, claims 1, 3-6, 8-13 and 15-28 are presented for examination.

Summary Of Examiner Interview

Applicants thank Examiner for granting an Examiner Interview on March 25, 2008. In the Examiner Interview proposed claim amendments were discussed, which are reflected in the newly amended claims. Examiner stated that a new prior art search would most likely be required in light of the claim amendments. No agreements were reached.

Information Disclosure Statement

Applicant acknowledges that patent numbers 5,582,717; 5,720,609; 5,721,222; 5,796,835 and 6,158,546 have not been reviewed by the Examiner. Regarding submitted reference DE 10004164A1, applicants have resubmitted this reference with an English translation of the Abstract.

Drawings

Applicant respectfully submits that the encryption key illustrated in block 206 of Fig. 2 is one example of unencrypted data. Therefore, the unencrypted data as recited in claims 1 and 13 is supported by the Figures.

Claim Objections

Claim 9 has been objected to for minor informalities. These informalities have been fixed.

Claim Rejections Under 35 U.S.C. § 112

Claims 1-24 are rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the enablement requirement. The claims are also rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically, the Office Action states:

> As per claims 1-2 and 13-14, "exchanging unencrypted data" and "wherein the exchanging of data include ... exchanging data encrypted with the encryption key" are being recited. In figure 2 of the original disclosure, it appears to the examiner that in step 206, encryption key is an unencrypted data transmitted to protected memory and in step 212, encryption data is transmitted to unprotected memory. However, in the independent claims, exchanging unencrypted data is being recited and in the dependent claims wherein the exchanging of data appears to the examiner is the exchanging of unencrypted data further includes exchanging of encrypted data, these two limitations are contradicted with each other and the original disclosure and therefore, they are not enabling.

(Office Action, 1/11/2008, page 5).

The claims have been amended to clearly distinguish between exchanging unencrypted data and exchanging encrypted data. Therefore, applicant respectfully submits that one of ordinary skill in the art would be able to practice the claimed invention in view of the specification. Applicant further submits that as amended the claims distinctly claim the subject matter which applicant views as an embodiment of the invention.

Double Patenting Rejection

The Examiner provisionally rejected claims 1, 2 and 13 on the ground of non-statutory obviousness-type double patenting as being unpatentable over claims 1, 2, 11, 15, 19 and 23 of copending application no. 10/977,158 (U.S. Publication No. 2006/0075259). Terminal disclaimers in compliance with 37 CFR § 1.321 are filed herewith to overcome the provisional non-statutory double patenting rejection.

Claim Rejections Under 35 U.S.C. § 103

Claims 1-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gehrmann et al. (US Pub. No. 2004/0176071, hereinafter "Gehrmann") in view of WO 01/75595 A2 (hereinafter "Ellison").

Claims 1, 3-6, 8-12, and 25-27

As amended, claim 1 recites:

> A method comprising:
> providing a trusted environment within a computer system for applications, the trusted environment including a protected section of memory that is inaccessible to direct memory access and an unprotected section that is accessible to direct memory access (pars. [0015], [0016]; Fig. 1);
> executing an application in the trusted environment (par. [0012]);
> providing a trusted path between the application and a SIM device that includes a SIM card, **the SIM device being physically connected with the computer system**, the trusted path being a path through a trusted port of a chipset included in the computer system, wherein the trusted port is mapped to the protected section of memory (pars. [0012], [0020], [0021]);
> providing an untrusted path between the SIM device and the application, the untrusted path being a path through an untrusted port of the chipset, wherein the untrusted port is mapped to the unprotected section of memory (par. [0026]);
> exchanging unencrypted data that includes an encryption key between the SIM device and the application via the trusted path, **wherein the**

unencrypted data to be exchanged is secured from unauthorized access via properties of the trusted path (pars. [0021], [0025]);

encrypting additional data using the encryption key (par. [0026]); and

exchanging the encrypted data between the SIM device and the application via the untrusted path (par. [0027]).

(citations to sections of the specification in which support for new limitations can be found has been added; emphasis added).

Gehrmann teaches providing wireless access of a SIM card to a remote client over an air interface. (Gehrmann, par. [0005]). In Gehrmann, the SIM card is included in a server communications device that is **wirelessly connected** to a remote client. (Gehrmann, par. [0050]). In contrast, claims 1 and 26 recite, "providing a trusted path between the application and a SIM device that includes a SIM card, the SIM device being **physically connected** with the computer system."

Gehrmann teaches a secure method for wirelessly transmitting data between a client and a SIM device of a server. (Gehrmann, par. [0001]). In Gehrmann, the data is secured using techniques that alter the data to place the data in a state that is unusable by any third parties that might intercept the data. Such techniques include use of shared secrets, public key pairs, a PIN number, encryption, or the like. (See, for example, Gehrmann, pars. [0021], [0022], [0057]). Each of the techniques for securing transmissions taught by Gehrmann are achieved by manipulating the data that is transmitted. In contrast, claims 1 and 26 recite, "wherein the unencrypted data to be exchanged is secured from unauthorized access via properties of the trusted path." Securing data by manipulating the data is not the same as securing data via properties of the trusted path.

Accordingly, Gehrmann does not teach or suggest at least the features of the present invention that are included in the following language of claim 1:

... providing a trusted path between the application and a SIM device that includes a SIM card, the SIM device being physically

> connected with the computer system, the trusted path being a path through a trusted port of a chipset included in the computer system, wherein the trusted port is mapped to the protected section of memory; ... exchanging unencrypted data that includes an encryption key between the SIM device and the application via the trusted path, wherein the unencrypted data to be exchanged is secured from unauthorized access via properties of the trusted path ...

Gehrmann also fails to teach or suggest at least the features of the present invention that are included in the following language of claim 26:

> ... providing a trusted path between the application and a SIM device that includes a SIM card, the SIM device being physically connected with the computer system, the trusted path being a path through a trusted port of a chipset included in the computer system, wherein the trusted port is mapped to the protected section of memory; ... exchanging unencrypted data between the SIM device and the application via the trusted path, wherein the unencrypted data to be exchanged is secured from unauthorized access via properties of the trusted path ...

Ellison teaches an isolated execution architecture for a computer system. (Ellison, page 4, par. 1). However, Ellison fails to teach the all of the limitations of claims 1 and 26 that are missing from Gehrmann.

Neither Ghermann nor Ellison, alone or in combination, teach or suggest all of the limitations of claim 1. Accordingly, applicants respectfully submit that the invention as claimed in claims 1 and 26, and their corresponding dependent claims, is patentable over the combination of Gehrmann and Ellison.

Newly added claims 25 and 27 recite, "determining, by the SIM device, that the application is executed in the trusted platform before exchanging the unencrypted data." Neither Gehrmann nor Ellison, alone or in combination, teach or suggest such a limitation. Accordingly, applicants respectfully submit that the present invention as claimed in claims 25 and 27 is patentable over the combination of Gehrmann and Ellison.

Claims 13 and 15-24

As amended, claim 13 recites:

> A system comprising:
> a system memory having a protected section that is inaccessible to direct memory access, an unprotected section that is accessible to direct memory access and a protected memory table that identifies the protected section and the unprotected section;
> a processor having a private cache memory that has protections that prevent access to said private cache memory by unauthorized devices, and registers that identify memory pages of the system memory that are accessible only to trusted code;
> a chipset having a trusted port mapped to the protected section of the memory and an unprotected port mapped to the unprotected section of the memory, the system memory, processor and chipset being components of a platform to provide a trusted environment for an application; and
> **a SIM device that includes a SIM card, the SIM device being physically connected with the platform**, to exchange unencrypted data that includes an encryption key with an application executed in the trusted environment via the trusted port, **wherein the unencrypted data to be exchanged is secured from unauthorized access by the trusted port**, and to exchange encrypted data with the application via the unprotected port.

(emphasis added).

Gehrmann teaches providing wireless access of a SIM card to a remote client over an air interface. (Gehrmann, par. [0005]). In Gehrmann, the SIM card is included in a server communications device that is **wirelessly connected** to a remote client. (Gehrmann, par. [0050]). In contrast, claim 13 as amended recites, "the SIM device being **physically connected** with the platform," wherein the platform includes the processor, client and memory.

Gehrmann teaches a secure method for wirelessly transmitting data between a client and a SIM device of a server. (Gehrmann, par. [0001]). In Gehrmann, the data is secured using techniques that alter the data to place the data in a state that is unusable by any third parties that might intercept the data. Such techniques include use of shared secrets, public key pairs, a PIN number, encryption, or the like. (See, for example, Gehrmann, pars. [0021], [0022], [0057]). Each of the techniques for securing transmissions taught by Gehrmann are

achieved by manipulating the data that is transmitted. In contrast, claim 13 has been amended to recite, "wherein the unencrypted data to be exchanged is secured from unauthorized access by the trusted port." Securing data by manipulating the data is not the same as securing data by a trusted port.

Accordingly, Gehrmann does not teach or suggest at least the features of the present invention that are included in the following language of claim 13:

> ... a chipset having a trusted port mapped to the protected section of the memory and an unprotected port mapped to the unprotected section of the memory, the system memory, processor and chipset being components of a platform to provide a trusted environment for an application; and
>
> a SIM device that includes a SIM card, the SIM device being physically connected with the platform, to exchange unencrypted data that includes an encryption key with an application executed in the trusted environment via the trusted port, wherein the unencrypted data to be exchanged is secured from unauthorized access by the trusted port, and to exchange encrypted data with the application via the unprotected port ...

Ellison teaches an isolated execution architecture for a computer system. (Ellison, page 4, par. 1). However, Ellison fails to teach the all of the limitations of claim 13 that are missing from Gehrmann.

Neither Ghermann nor Ellison, alone or in combination, teach or suggest all of the limitations of claim 13. Accordingly, applicants respectfully submit that the invention as claimed in claim 13, and its corresponding dependent claims, is patentable over the combination of Gehrmann and Ellison.

Conclusion

Accordingly, Applicant respectfully requests the withdrawal of the rejections and submits that pending claims 1, 3-6, 8-13 and 15-28 are in condition for allowance. Applicant respectfully requests reconsideration of the application and allowance of the pending claims.

If the Examiner determines the prompt allowance of these claims could be facilitated by a telephone conference, the Examiner is invited to contact Benjamin Kimes at (408) 720-8300.

Deposit Account Authorization

Authorization is hereby given to charge our Deposit Account No. 022666 for any charges that may be due. Furthermore, if an extension is required, then Applicant hereby requests such extension.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: 4/11/08

/Benjamin A. Kimes/
Benjamin A. Kimes
Reg. No. 50,870

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(408) 720-8300